UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/643,564 | 08/18/2003 | Bruce McCorkendale | SYMC1032 | 4932 |

34350 7590 07/10/2008

GUNNISON, MCKAY & HODGSON, L.L.P.
1900 GARDEN ROAD, SUITE 220
MONTEREY, CA 93940

| EXAMINER | |
|---|---|
| KHOSHNOODI, NADIA | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2137 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 07/10/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/643,564 | MCCORKENDALE ET AL. | |
| | Examiner | Art Unit | |
| | NADIA KHOSHNOODI | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *04 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,3,5-11 and 15-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,5-9, 15-19, 26-28* is/are rejected.

7)☐ Claim(s) *10-11, 20-25* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Amendment*

Claims 2, 4, and 12-14 are cancelled. Applicant's arguments/amendments with respect to claims 1, 3, 5-9, and 26-28 filed 4/4/2008 have been fully considered and are therefore rejected under new grounds. Arguments with respect to claims 15-19 have been considered but are not persuasive. Finally, claims 10-11 and 20-25 are herein indicated as having allowable subject matter. Examiner would like to point out that this action is made final (See MPEP 706.07a).

### *Allowable Subject Matter*

Claims 10-11 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 20-25 are allowed.

The following is a statement of reasons for the indication of allowable subject matter: the limitations regarding buffering outbound traffic and then comparing the buffered outbound traffic to the copied inbound traffic in order to determine if malicious code has been detected are not fairly taught/suggested by the prior arts of record.

### *Response to Arguments*

Applicants contend that Chesla et al. fail to teach/suggest "comparing at least a portion of the copied inbound traffic with at least a portion of copied outbound traffic." Examiner respectfully disagrees. Chesla et al. teach that copies are first maintained in trap buffers to allow

further scrutiny of the incoming/outgoing traffic (paragraphs 240, 300, and 365). Chesla et al. further teach that the unfiltered traffic received, i.e. inbound traffic, and the filtered traffic, i.e. outbound traffic are compared in order to determine whether or not there is a potential attack (par. 137). Furthermore, in another section, Chesla et al. also teach that the number of inbound packets are compared with a number of outbound packets where the result is used in order to determine the likelihood that an attack is underway (par. 236-237). Finally, Chesla also teach that the arrival times of a previous message that was received and transmitted, i.e. outbound traffic, is compared with the arrival time of a new message that is received, i.e. inbound traffic, in order to determine whether or not an attack is underway (par. 301). Examiner would like to note that Applicants have not specifically defined what inbound and what outbound traffic are compared, thus the Examiner has broadly interpreted (according to MPEP 2111) inbound traffic to mean recent traffic which has been received by the system and outbound traffic to mean traffic which is or has recently been sent/distributed. Thus, the Examiner maintains that Chesla et al. teach comparing at least a portion of the copied inbound traffic with at least a portion of copied outbound traffic.

Due to the reasons stated above, the Examiner maintains rejections with respect to the pending claims. The prior arts of records taken singly and/or in combination teach the limitations that the Applicant suggests distinguish from the prior art. Therefore, it is the Examiner's conclusion that the pending claims are not patentably distinct or non-obvious over the prior art of record as presented.

***Claim Rejections - 35 USC § 103***

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 3, 5-7, and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini et al., US Pub. No. 2003/0101353 and further in view of Pak et al., US Patent No. 7,080,408.

As per claims 1 and 26:

Tarquini et al. substantially teach a method/computer program product comprising a computer readable medium configured to store code, the method/computer program product comprising: comparing at least a portion of outbound traffic on a host computer system to at least a portion of inbound traffic on the host computer system, wherein the inbound traffic is received on the host computer system from a source external to the host computer system (par. 48, lines 1-32) and wherein the outbound traffic is generated on the host computer system for transmission from the host computer system to a destination external to the host computer system, and further wherein the at least a portion of the outbound traffic is subsequent in time to the at least a portion of the inbound traffic (par. 48, lines 1-32); and determining an attack is detected on the host computer system based on the comparing (par. 48, lines 15-32); when an attack is detected, providing a notification of the attack detection (par. 48, lines 32-46).

Not explicitly disclosed is wherein the type of attack detected is that of detecting malicious code. However, Pak et al. teach that incoming/outgoing traffic may be monitored in

order to detect various attacks on the host, such as detecting malicious code received from an external source (col. 4, lines 16-44). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Tarquini et al. to monitor the host computer for malicious code. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Pak et al. suggest that early detected of malicious code helps prevent damage to a network in col. 2, lines 21-23.

As per claim 3:

Tarquini et al. and Pak et al. substantially teach the method of claim 1. Furthermore, Pak et al. teach the method wherein the comparing is performed using a similarity comparison technique (col. 5, lines 15-33).

As per claim 5:

Tarquini et al. and Pak et al. substantially teach the method of claim 1. Furthermore, Tarquini et al. teach the method wherein the inbound traffic is received at the host computer system from a source port, and wherein the outbound traffic is for sending to a destination port, and further wherein the source port and the destination port are the same port (par. 44).

As per claim 6:

Tarquini et al. and Pak et al. substantially teach the method of claim 1. Furthermore, Pak et al. teach the method wherein the inbound traffic is received on the host computer system from a source port, and wherein the outbound traffic is for sending to a destination port, and further wherein the source port and the destination port are different ports (col. 5, lines 20-28).

As per claim 7:

Tarquini et al. and Pak et al. substantially teach the method of claim 1. Furthermore, Pak et al. teach the method further comprising: implementing protective actions (col. 5, lines 39-47).

As per claim 27:

Tarquini et al. and Pak et al. substantially teach the computer program product of claim 26. Further Pak et al. teach wherein the comparing is performed using a similarity comparison technique (col. 5, lines 15-33).

As per claim 28:

Tarquini et al. and Pak et al. substantially teach the computer program product of claim 26. Furthermore, Pak et al. teach the computer readable medium configured to store computer program code further comprising: implementing protective actions (col. 5, lines 39-47).

III. Claims 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini et al., US Pub. No. 2003/0101353 and Pak et al., US Patent No. 7,080,408 as applied to claim 1 above, and further in view of Chesla et al., US Pub. No. 2004/0250124.

As per claim 8:

Tarquini et al. and Pak et al. substantially teach the method of claim 1. Pak et al. further teaches that a message digest may be stored when the traffic is intercepted (col. 6, lines 4-19). Pak et al. also further teach that a copy of data may be quarantined and that copy may be used instead of the original data received in detecting malicious code, i.e. intercepting the inbound traffic; copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic; releasing the inbound traffic (col. 5, lines 39-47). Not explicitly disclosed is the method further comprising: intercepting the outbound traffic; copying the outbound traffic to an outbound traffic memory area, the copying the outbound traffic

generating copied outbound traffic; and releasing the outbound traffic. However, Chesla et al. teach that copies of values of the incoming traffic/outgoing traffic may be stored in both inbound and outbound directions in order to allow for detecting possible attacks. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Tarquini et al. and Pak et al. to store a copy of the inbound and outbound traffic in different memory areas in order to determine if a possible flooding attack (as one example) is underway. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Chesla et al. suggest that using a list of incoming/outgoing signatures and monitoring that list closely (while still releasing the traffic) provides a great technique for various attack detections on a network in par. 353-355.

As per claim 9:

Tarquini et al., Pak et al., and Chesla et al. substantially teach the method of claim 8. Furthermore, Chesla et al. teach wherein the comparing comprises: comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic.

IV. Claims 15-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chesla et al., US Pub. No. 2004/0250124 further in view of Hoepers et al., "Honeynets Applied to the CSIRT Scenario.".

As per claim 15:

Chesla et al. substantially teach a method comprising: intercepting inbound traffic on a host computer system, wherein the inbound traffic is received on the host computer system from a source external to the host computer system (par. 121); copying the inbound traffic to an

inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic (par. 365-370); releasing the inbound traffic (par. 353-355); intercepting outbound traffic on the host computer system(par. 149); copying the outbound traffic to an outbound traffic memory area, the copying the outbound traffic generating copied outbound traffic (par. 300); releasing the outbound traffic (par. 353-355); comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic (par. 137); determining if malicious code is detected on the host computer system based on the comparing (par. 137); and if malicious code is detected, providing a notification of the malicious code detection (par. 435).

Not explicitly disclosed is wherein the outbound traffic is generated on the host computer system for transmission from the host computer system to a destination external to the host computer system. However, Hoepers et al. teach that outgoing traffic generated on a host machine which are not in response to an incoming packet received are captured and an alert for interception of malicious traffic is generated. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chesla et al. to compare the outgoing traffic to determine whether or not it is in response to incoming/received traffic in order to create an alert when the outgoing traffic is generated on the host machine is not in response to any of the received/incoming traffic. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Hoepers et al. suggest that generating an alert for outgoing traffic generated without being a response to incoming traffic will help lessen the impact that malicious traffic has on a network on page 5, section 2.4.1, number 1.

As per claim 16:

Chesla et al. and Hoepers et al. substantially teach the method of Claim 15. Furthermore, Chesla et al. teach wherein the comparing is performed using a similarity comparison technique (par. 159).

As per claim 17:

Chesla et al. and Hoepers et al. substantially teach the he method of claim 15. Furthermore, Chesla et al. teach wherein the at least a portion of the copied outbound traffic is subsequent in time to the at least a portion of the copied inbound traffic (par. 159).

As per claim 18:

Chesla et al. and Hoepers et al. substantially teach the method of claim 15. Furthermore, Chesla et al. teach the method further comprising: prior to the copying the outbound traffic, if the outbound traffic correlates to a prior name resolution lookup performed on the host computer system, releasing the outbound traffic (par. 134 and 289).

As per claim 19:

Chesla et al. and Hoepers et al. substantially teach the he method of claim 15. Furthermore, Chesla et al. teach wherein the inbound traffic is copied to the inbound traffic memory area on a per port basis (par. 189), and wherein the outbound traffic is copied to the outbound traffic memory area on a per destination port basis (par. 295).

*References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Pub. No. 2003/0154255
2. US Pub. No. 2006/0212572
3. US Pub. No. 2003/0074578
4. US Patent No. 6,925,572
5. US Pub. No. 2004/0111531
6. US Pub. No. 2002/0032871 - state of the art suggesting that intrusion detection systems often use copied data in identifying malicious attacks

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/Nadia Khoshnoodi/
Examiner, Art Unit 2137
7/6/2008

NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137